ATTACHMENT C

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

Yahoo!
701 First Avenue
Sunnyvale, California 94089

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER: 13-223-M

I, **Adam Sucheski**, being duly sworn, depose and say:

I am a(n) **Special Agent of the Federal Bureau of Investigation ("FBI")** and have reason to believe that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

SEE ATTACHMENT "A"

there is now concealed a certain person or property, namely
(describe the person or property to be seized)

SEE ATTACHMENT "B"

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

property designed/intended for use or which is or has been used as the means of committing a crime, evidence of commission of a crime, fruits of a crime

concerning a violation of Title **18**, United States Code, Section(s) **2251, 2252 and 2252A**.
The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant

Sworn to before me, and subscribed in my presence

2/21/13
Date

Philadelphia, PA
City and State

HONORABLE M. FAITH ANGELL, U.S. Magistrate Judge
Name and Title of Issuing Officer

Signature of Issuing Officer

ATTACHMENT C

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

SEARCH WARRANT

Yahoo!
701 First Avenue
Sunnyvale, California 94089

CASE NUMBER: 13-223-M

TO: **Agents of the Federal Bureau of Investigatin ("FBI")** and any Authorized Officer of the United States

Affidavit(s) having been made before me by **Adam Sucheski** who has reason to believe that ☐ on the person of or ☒ on the property or premises known as (name, description, and/or location)

SEE ATTACHMENT "A"

there is now concealed a certain person or property, namely
(describe the person or property)

SEE ATTACHMENT "B"

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before _____
Date

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime – 6:00 A.M. to 10:00 P.M.) ~~(at any time in the day or night as I find reasonable cause has been established)~~ and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to **HONORABLE M. FAITH ANGELL**, United States Magistrate Judge as required by law.

2/21/13 11:40 AM
Date and Time Issued

Philadelphia, PA
City and State

HONORABLE M. FAITH ANGELL, U.S. Magistrate Judge
Name and Title of Issuing Officer

Signature of Issuing Officer

AO 93 (Rev. 5/85) Search Warrant

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned to me this date.

HONORABLE M. FAITH ANGELL
U.S. Magistrate Judge

Date

13-223-M

AFFIDAVIT

I, Adam Sucheski, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), Philadelphia Division, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of the FBI for seven years, and am currently assigned to the Philadelphia Division's Fort Washington Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to child pornography, robbery and securities fraud. I have gained experience through training at the FBI Academy and prior law enforcement training.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The statements in this Affidavit are based on my investigation and other law enforcement officers investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2252, 2252A, and 2251, are located at Yahoo! 701 First Avenue, Sunnyvale, California and are associated with email addresses xtictac22@yahoo.com and yourfantasy1207@yahoo.com.

LEGAL AUTHORITY

4. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor

engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

5. Title 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

6. Title 18 U.S.C. § 2251(a) prohibits a person from using the mail or any facility, including the computer, or means of interstate or foreign commerce, from knowingly employing, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

7. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Yahoo. I request that Yahoo be required to produce the electronic communications and other information identified in Attachments A and B hereto. Because Yahoo is not aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Yahoo to perform the search would be a burden upon the company. If all Yahoo is asked to do is produce all the files associated with the account, an employee can do that

easily. Requiring Yahoo to search the materials to determine what content is relevant would add to their burden.

8. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B from what is produced by Yahoo pursuant to the search warrant. In reviewing these files, I will treat them in the same way as if I were searching a file cabinet for certain documents. E-mails will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

9. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

10. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Yahoo to comply even though Yahoo is not located in this district, because the Court has jurisdiction over the offense being investigated.

11. I also ask that the warrant direct Yahoo to produce records and other information pertaining to this account. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth below to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

DEFINITIONS

7. The following definitions apply to this Affidavit:

a. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see Title 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See Title 18 U.S.C. § 2256(5)).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the

same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See Title 18 U.S.C. § 2256(2)).

e. "Computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Minor" means any person under the age of eighteen years. (See Title 18 U.S.C. § 2256(1)).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and colocation of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e mail address," an e mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by

using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

h. "Domain names" are common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top-level domains, are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world-wide web server located at the United States Department of Justice, which is part of the United States government.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses

the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

j. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. (See Title 18 U.S.C. 2510(15)).

k. "MD5 Hash Value", also known as a message digest, is a mathematical value generated by applying an algorithm to a computer file that is represented by a sequence of 32 hexadecimal digits. Among computer forensics professionals, the MD5 hash value is generally considered to be a unique signature or fingerprint for a file.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, E-MAIL, AND FACEBOOK

8. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information.

9. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

10. E-mail is a popular form of transmitting messages and or files in an electronic

environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

11. Internet-based e-mail is a service provided by an electronic communication service provider allowing individuals to send and receive e-mail from any Internet connected computer, regardless of their location or Internet service provider (ISP). Individuals utilizing Internet-based e-mail services access their accounts by "logging in" through the web-browser software installed on their computer, often by providing an account name and an associated password. Once the service provider's computers have determined the password is correct for the given account name, the individual "logged-in" can access any e-mail sent to their account, and or send e-mail to any other e-mail address accessible via the Internet.

12. Internet-based e-mail service providers reserve and or maintain computer disk storage space on their computer system, usually limited and closely regulated, for the use of the service subscriber for the storage of e-mail communications with other parties, which include graphic files, programs, or other types of date stored in electronic form.

13. Internet-based e-mail service providers maintain records pertaining to the individuals Who subscribe to their services. These records could include the account holder's name, address, date of birth, gender, occupation, and the Internet Protocol (IP) address used to establish the account and subsequent accesses to that account.

14. Any e-mail that is sent to a Internet-based e-mail subscriber is stored in the subscriber's

"mail box" on the electronic communications service provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the provider. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely. Electronic communications service providers can also perform backups of subscriber's email accounts as routine maintenance in case their servers become inoperable so the content in the subscriber's account is not lost.

15. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. Most Internet-based e-mail users have the option of saving a copy of a sent e-mail. Unless the sender of the e-mail specifically deletes the e-mail from the provider's server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained by the provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations.

16. Internet-based e-mail provider's typically offer services to their subscribers that allow them to store any electronic file (i.e. image files, text files, etc.) on servers maintained and or owned by the provider.

17. E-mails and other electronic files stored on an electronic communications service provider's server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and or which he/she does not wish

to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the provider's server.

12. Yahoo's e-mail is an Internet-based electronic communications system operated by Yahoo. It permits its users to communicate using e-mail and other methods such as instant messenging. Instant Messenging allows users to have direct and private chat conversations with other users of that service.

18. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four

functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now convert photographs onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTOR

19. I know from my training, experience, and information provided to me by other investigators that the following characteristics are prevalent among individuals who collect child pornography:

a. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography collect explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their sexual fantasies involving children.

c. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer, e-mail, bulletin boards, Internet relay chat, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or on scraps of paper.

f. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage.

g. Recent studies have shown that those who collect child pornography are more likely to be "contact offenders" with children. In a study published in the Journal of Abnormal Psychology, Vol. 15, No. 3, pp. 610-615, by Seto, Cantor, and Blanchard, titled "Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia," the authors concluded an interest in child pornography is a strong indicator of pedophilia. In December, 2010, Seto, Hanson, & Babchishin, published an article entitled "Contact Sexual Offending by

Men With Online Sexual Offenses," in Sexual Abuse: A Journal of Research and Treatment. This article was a meta-analysis of a number of studies of possessors of child pornography. This was a meta-analysis of 24 studies of possessors of child pornography. In the studies that relied only upon subsequent arrests and/or convictions, the number of contact offenses with children ran from 4.6% to 13.3%. In the three studies in which the subjects were subject to polygraph examinations, the percentages ranged from 32.3% to 84.5%, with the middle study finding 55.3%. In the remaining three studies which relied only upon self-reporting, the numbers ranged from 32.8% to 57.4%. Each of the last three studies was unique. In Neutze, Seto, Schaefer, Mundt, & Beier (in press at this time), the subjects were in Germany. They had sought counseling on their own and were not referred by the criminal justice system. In the venue where the study was conducted, therapists were not legally required to report the admissions of their subjects (36.5%). In Quayle & Taylor (2003), the number of subjects was sample small (23) and had established good rapport with the therapists (47.8%). Finally, in Coward, Gabriel, Schuler, and Prentky (2009), the subjects reported anonymously (32.8%). In performing their statistical analysis of these studies, Seto, Hanson, & Babchishin concluded that more than 50% of those convicted of "possession only" admitted to at least one contact offense, when one relied on more than an arrest or conviction for a new offense.

BACKGROUND OF THE INVESTIGATION

20. On October 18, 2012, your Affiant was provided information from Facebook which appeared to indicate that a twenty-seven year old man was involved in the enticement and production of child pornography. Facebook had discovered suspected sexual conversations between a adult male and a minor female. Facebook notified the National Center for Missing

and Exploited Children (NCMEC) who subsequently advised the FBI. Your Affiant was advised that Facebook user WENDELL LANDIS, user identification (UID) 1641165072 had his profile disabled by Facebook as it appeared that he was violating their terms of service for engaging in sexual conversation with a minor. Facebook provided a telephone number for the suspected minor as well as her Facebook UID and IP address information.

21. Through public records checks and law enforcement databases, your Affiant identified WENDELL LANDIS as ROBERT WENDELL LANDIS, date of birth December 7, 1984. Your Affiant also located an active Facebook account for LANDIS, bearing vanity name wlandis1. On this Facebook webpage, LANDIS indicates that he works for Exton Nissan, in Exton, Pennsylvania. Your Affiant has viewed the photographs from the active Facebook page as well as LANDIS' Pennsylvania driver's license photograph. Your Affiant believes that they are the same individual, ROBERT WENDELL LANDIS.

22. Your Affiant reviewed the information from Facebook, which provided several IP addresses from which LANDIS accessed his account. The most recent in the records was 173.12.13.209 assigned on 07/20/2012 00:38:27 UTC

23. Your Affiant reviewed the information provided and located telephone number 215-262-4363 within the records for UID 1641165072. Your Affiant sent a subpoena to Verizon, which indicated that the telephone number is assigned to ROBERT W. LANDIS, 1507 Salford Street, Salford, PA 18957. A review of toll records provided by Verizon indicates that LANDIS had telephonic contact 79 times with the minor[1] between January 1, 2012 and October 21, 2012.

24. Your Affiant reviewed the information provided and located IP address 75.131.214.244

[1] The mother of the minor confirmed the telephone number known to your Affiant, which had been provided by Facebook was the telephone number utilized by her minor daughter.

within the information for the suspected minor. The IP address was assigned on 10/7/2012 at 19:56:19 UTC and was utilized to access the minor's Facebook account. Your Affiant sent a subpoena to Charter Communications for information on the IP address.

25. On November 2, 2012, your Affiant received a response to a subpoena from Charter Communications. Charter Communications advised that IP address 75.131.214.244 was assigned to an account holder at an address known to your Affiant in Buford, Georgia on 10/7/2012 at 19:56:19 UTC. Through public records checks, your Affiant located and spoke with the account holder on November 7, 2012. The account holder indicated that her daughter is a minor, born in 1996 and that she had lived in Chester County, Pennsylvania up until July 2012, when they moved to Buford, Georgia. Her daughter's Facebook account is associated with UID 1334013414.

26. On November 6, 2012, Comcast responded to a subpoena for records related to IP address 173.12.13.209 assigned on 07/20/2012 00:38:27 UTC. The records indicate that this IP address is a statically assigned IP address, the subscriber is EXTON NISSAN, 200 West Lincoln Highway, Exton, Pennsylvania 19341. Additionally, Comcast advised that email address rlandis325@comcast.net is assigned to ROBERT LANDIS, 1102 Colonial Court, Norristown, Pennsylvania 19403, with telephone number 215-262-4363.

27. On November 8, 2012, Hotmail Inc. responded to a subpoena for records related to xtictac22@hotmail.com. This email address was provided by Facebook as an alternate contact associated with LANDIS' Facebook account UID 1641165072. The records indicate that xtictac22@hotmail.com is registered to RW Landis, Pennsylvania, 18957 with the last IP login of 98.225.253.10 on 10/20/2012 4:08:32 AM (PDT). An additional IP address was utilized on

10/19/2012 4:20:52 PM (PDT) 173.12.13.209. This address has been identified as the static IP address assigned to Exton Nissan.

28. Your Affiant subpoenaed records related to IP address 98.225.253.10 on 10/20/2012 4:08:32 AM (PDT), which is assigned to CellCo DBA Verizon Wireless.

29. On December 4, 2012, your Affiant spoke with an employee of the property management company responsible for 1102 Colonial Court, Norristown, Pennsylvania. The representative advised that ROBERT LANDIS has signed a lease for 1102 Colonial Court for one year. The period of the lease is November 14, 2012 to November 14, 2013. The employee further noted that telephone number 215-262-4363 and email address rlandis325@comcast.net were on file as methods of contact. LANDIS' unit also has a parking space associated with it. Your Affiant observed a white Nissan sedan, bearing Pennsylvania registration K02212K, parked in LANDIS' assigned space. The vehicle registration is a dealer plate issued to Chester County Nissan DBA Exton Nissan, 200 West Lincoln Highway, Exton, Pennsylvania 19341.

30. On December 4, 2012, your Affiant contacted the Montgomery County 911 center and requested an address check for 1102 Colonial Court, Norristown, Pennsylvania. The 911 operator indicated that the property is in West Norriton Township[2].

31. On December 5, 2012, the previously identified minor (paragraph 22 herein) was interviewed by a child victim specialist, and was observed by a FBI Special Agent assigned to the Atlanta Division. During the interview, the minor indicated that she did know LANDIS (as WENDELL) and that she had engaged in sexual activity with him on multiple occasions. The minor stated that she engaged in oral, anal, and vaginal sex with LANDIS. The minor further indicated that she was still in telephonic and Facebook contact with LANDIS. The minor

[2] The address is in West Norriton Township, but may utilize a Norristown mailing address.

retrieved LANDIS' previously identified telephone number from her cell phone and provided it to investigators.

32. On December 3, 2012, your Affiant served a search warrant on Facebook Inc. for records related to LANDIS' closed and current Facebook account. On December 13, 2012, those results were received and reviewed.

33. A review of the records for Facebook UID wlandis1 indicates that the date of birth supplied for the account is December 7, 1984, which is LANDIS' date of birth. An email address of rlandis325@comcast.net was supplied as a means of contact.

34. Additionally, between November 15, 2012 and November 27, 2012, the user has used an Apple iPad or Apple iPhone device to access the Facebook account from IP addresses 98.225.253.10. This IP address has been identified as assigned to Robert Landis.

35. A review of the records for Facebook UID 1641165072 indicates that the date of birth supplied for the account is December 7, 1984, which is LANDIS' date of birth. An email address of xtictac22@hotmail.com was supplied as a means of contact. This email address was previously identified as belonging to LANDIS.

36. Your Affiant reviewed the messages provided by Facebook between LANDIS and the previously identified minor and noted the following conversations. A conversation on April 29, 2012 at approximately 6:00 PM is as follows: Wendell Landis (WL) and Minor (M) WL:

"Lol...I wanna take pics of u..."

M "Nnnn what kindd ;)"

WL "Not ones u can put on fb... Maybe start out with underwear pics..."

M "Mmm u can take any type u want ;)'

WL "Maybe end up takin pics of u sucking my dick... or maybe a pic of my dick in ur ass..."

M "Anything you want hun."

WL "We need a day where ur home alone..."

M "We doo uhmmm I can get outta school at 12, one day if I need too ;)"

WL "Thursday?"

M "I can tryy"

WL "Will ur mom be home?"

40. The conversation continues and LANDIS asks the minor if she will be able to leave the house with her parents' permission and falsely indicates that he is 18 years old. LANDIS also appears to indicate that he is aware of the legal issues with their age differences and sexual contact:

WL "Would ur parents let u go back to my place?"

M "Lol noo they wouldnt noee"

WL "We can't do that ...be I'm 18 there's too many legal things there...."

41. LANDIS and the minor discuss sending and receiving photographs in the past and the minor indicates that she can provide LANDIS with a micro SD card with photos on it. The minor will provide the photos to LANDIS on this card, and he can transfer them to his cellular telephone.

42. As the conversation continues, it appears to show LANDIS is planning to meet the minor;

WL "I gotta make sure I can come tonight."

M "Okayyss well if u can. U can do w,e u want to me and take any pics u want ;)"

WL "I wanna finger ur ass while u suck my dick."

M "Go ahead ;)"

43. Approximately two hours later, LANDIS and the minor discussing what occurred during a prior encounter;

M "Haha not uhh! I jus kissed u alott"

WL "That's all?"

M "At first haha hten u were like I gotta stop or im guna wanna fuck u haha."

WL "So u kept going..."

M "Hahaha I did ;) hey im not the one who gets excited that easilyy loll all we didw eas make out and u were ROCK hard."

WL "R u complaining?"

M "U acted rlly surpriseedd when I sat on u lol I toldd u I was rlly tight :P I hope u liked it thooo ;)"

WL "It felt good."

M "Well if u come ovr then u can feel it again."

WL "u sure?:"

M "100% sure ;) and maybe this timee u can take some control when we fuck ;) and last longer."

44. On May 1, 2012, LANDIS emails the minor and again asks for photographs to be sent to him. The minor indicated that she was unable to get on the computer at school. During the conversation, the minor asks what LANDIS' email is. LANDIS indicates xtictac22@yahoo.com.

45. On May 5, 2012, LANDIS and the minor appear to be planning to meet the next day;

WL "R ur parents gonna be home al day tomorrow?"

M "Yeahh but I can jus go to the park."

WL "idk if I can fuck but would love a nice bj."

46. On May 6, 2012, it appears that LANDIS and the minor planned to meet after the minors parents go to sleep:

WL "R u horny?'

M "Mmhhmmm"

WL "My back and neck r killing me."

M ":(im sorryy im on my way down now."

47. On May 16, 2012, the minor indicates that her friends doubt that LANDIS is 18 years of age, possibly older like 20 or 21 years old. LANDIS indicates that he is not 20 or 21. During the conversation on this date, LANDIS indicates that he utilizes his iPad to access Facebook all day.

48. On December 21, 2012, your Affiant executed a search warrant on LANDIS' residence and seized multiple computer devices, including iPhones, iPad, and laptop computers. Further analysis by the Philadelphia Regional Computer Forensics Lab (RCFL) of these devices yielded additional data.

49. LANDIS was interviewed on the date of the search and indicated that he has never enticed or attempted to entice a minor to take photographs of him or herself. LANDIS has never had sex

with a minor. LANDIS does not have any known minors as contacts in his telephone or e-mail. LANDIS stated that he never talked with a minor on Facebook, nor attempted to entice a minor on Facebook. LANDIS also provided the following e-mail addresses which he uses or has used in the past; wlandis@extonnissan.com, rlandis325@comcast.net, xtictac22@hotmail.com, xtictac22@gmail.com, xtictac22@yahoo.com, yourfantasy1207@yahoo.com, rwcycles@gmail.com. LANDIS indicated he rarely uses the Yahoo! addresses, but does occasionally check them.

50. On February 11, 2013, your Affiant received the full reports from the RCLF related to the analysis of an iPhone, iPad, and laptop computer utilized by LANDIS. The data indicates that the previously identified minor's email address and telephone number were stored within the iPad and iPhone. The recovered data further indicated that the iPad was used to type in "Buford" and the name of the account holder previously noted in paragraph 25.

51. The data recovered from the RCFL indicates that LANDIS' Gateway laptop was utilized to access Yahoo! Mail on numerous occasions, most recently on the following dates, August 14, 2012, August 28, 2012, September 1, 2012, October 16, 2012, and December 17, 2012. The data also indicates that LANDIS utilizes cloud storage to move and download photographs.

52. Your Affiant also reviewed photographs recovered from LANDIS' iPhone and observed approximately ten photographs of the minor female noted above. The photographs show the minor with exposed breasts, exposed genitalia, as well as wearing a bra and underwear. The photographs have been sent to the Atlanta Division to be identified by the minor's mother.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

48. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an

operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

49. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media). In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the crime(s), within the meaning of Title 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

To search for electronic data contained in computer hardware, computer software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. searching for image files to locate images of children engaging in sexually explicit conduct, examining log files associated with the receipt, transmission, and viewing of such images, and examining all of the data contained in such computer hardware, computer software, and /or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. surveying various file directories and the individual files they contain;

c. on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s).

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

h. searching for malware in order to evaluate defenses, such as viruses; and/or

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

50. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently-viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

CONCLUSION

51. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that ROBERT WENDELL LANDIS has knowingly persuaded, induced, enticed, or coerced a minor to engage in sexually explicit conduct for the purpose of producing visual depictions of such conduct, and received and or possessed child pornography, and respectfully submits that there is probable cause to believe that there is evidence of the commission of criminal offenses by ROBERT WENDELL LANDIS, namely, violations of Title 18, United States Code, Sections 2252, 2252A, and 2251, located at Yahoo! 701 First Avenue, Sunnyvale, California and associated with email addresses xtictac22@yahoo.com and yourfantasy1207@yahoo.com and this evidence, listed in Attachments A and B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

52. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachments A and B.

Adam Sucheski
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 27 day of February, 2013.

HONORABLE M. FAITH ANGELL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
(To Be Served Upon Yahoo)

Location to be searched: Yahoo, 701 First Avenue, Sunnyvale, California, and other locations where Yahoo servers are located that store e-mail and user account content and information.

Items to be Seized (xtictac22@yahoo.com and yourfantasy1207@yahoo.com):

A. Preserved data requested on December 13, 2012 via Preservation Letter , Yahoo! internal reference number 221568 which included all content stored in or associated with e-mail accounts xtictac22@yahoo.com and yourfantasy1207@yahoo.com to include e-mails (read, sent, deleted, draft, and unopened) whether in a mailbox, user created folders, or other storage locations, attachments, documents, graphics, and any other uploaded, saved, or associated files;

B. histories;

C. buddy lists, contacts, address books;

D. profiles;

E. subscriber information;

F. method of payments;

G. detailed billing records (log on and log off times);

H. terms of service violations;

I. and IP connection data; all in relation to e-mail account xtictac22@yahoo.com and yourfantasy1207@yahoo.com

ATTACHMENT B
(To be executed by Law Enforcement Agents)

Items to be seized:

All files, documents, communications, and contacts associated with the account xtictac22@yahoo.com and yourfantasy1207@yahoo.com related to the production, receipt, distribution, and or possession of files of minors engaging in sexually explicit conduct and or sadistic or masochistic abuse, to include child pornography; visual depictions of minors engaging in sexually explicit conduct; communications about or to minors; and any contact with minors; in violation of Title 18, United States Code, Sections 2252, 2252A and 2251, along with any evidence that would tend to show the true identities of the persons committing these offenses.

All available log files showing dates, times and IP addresses for access to this account.